



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/792,062	03/02/2004	Jun Wang	030157	4204

23696 7590 11/20/2009  
QUALCOMM INCORPORATED  
5775 MOREHOUSE DR.  
SAN DIEGO, CA 92121

EXAMINER
----------

DESIR, PIERRE LOUIS

ART UNIT	PAPER NUMBER
----------	--------------

2617

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

11/20/2009

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com  
kascanla@qualcomm.com  
nanm@qualcomm.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/792,062	<b>Applicant(s)</b> WANG ET AL.	
	<b>Examiner</b> PIERRE-LOUIS DESIR	<b>Art Unit</b> 2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 28 July 2009.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1,3-5,7-18,20,22-26 and 28-45 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3-5,7-18, 20 and 22-26, 28-45 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments with respect to claims 1,3-5,7-18,20,22-26 and 28-45 have been considered but are moot in view of the new ground(s) of rejection.

Applicants argue that Rowitch does not describe performing both authorization as well as authentication of location determination based on the first security procedure. To support this argument, Applicants state that the abstract from Rowitch mentions authorization of location determination but is silent as to authentication. Additionally, continue applicants, the abstract from Rowitch does not describe using the same first security procedure for authentication of location determination.

Examiner respectfully disagrees.

Rowitch describes a system, method and apparatus for providing location services whereby location determination and location disclosure are treated as separate and independent processes. Location determination may be performed via a first set of network entities to obtain location information for a mobile station. Location determination may utilize a first security procedure for authorization and to obtain a first session key used for location determination (see abstract). Thus, through only a first security procedure, authorization and authentication (i.e., used of a session key) are performed for location determination.

Applicants also argue that Rowitch describes authorization of location disclosure based on a second procedure, but is silent as to authentication. Rowitch, continue applicants, does not described using the same second security procedure for authentication of location disclosure.

Art Unit: 2617

Again, Examiner respectfully disagrees.

Rowitch discloses that location disclosure may utilize a second security procedure for authorization and to obtain a second session key used for location disclosure. Thus, it is clear that through the second security procedure, authorization and authentication (i.e., the obtaining of a second session key) are performed for location disclosure. Examiner wants to respectfully refers applicants to claims 1-5 of Rowitch for further evidences.

The above response also applies to claims 18, 30, and 44.

Regarding claim 22, Applicants argue that Rowitch does not describe a mobile station that includes a function that interacts with a second peer function in a network entity that is distinct from the function in the network entity that interacts with the mobile station to obtain location information. Nor does it disclose operation of location disclosure to the mobile station.

First, it should be noted that the claim does not disclose, “the operation of location disclosure to the mobile station.” The claim, however, does describe “providing location information for the mobile station.”

And, paragraphs 24-26, 36-37, do describe location determination procedure through an interaction between the mobile station and a second network entity, peer function or otherwise. Therefore, as written, Rowitch does read on claim 22.

The above response also applies to claim 23.

**Regarding claims 24 and 29, Applicants argue that Rowitch does not disclose authentication and encryption of messages using session key.**

**Applicants’ arguments are persuasive. New ground of rejection has been applied.**

**Regarding claim 35, Applicants' arguments are persuasive. New ground of rejection has been applied.**

Regarding claims 36 and 43, Applicants argue that Rowitch does not describe limiting any session key to a home network to a home network.

Examiner respectfully disagrees.

First it should be noted that the specification provides no support for such disclosure. Therefore, a new matter rejection will be applied. And such disclosure will be interpreted as understood by examiner.

As disclosed above, Rowitch discloses that location disclosure utilizes a second session key utilize a second security procedure for authorization and to obtain a session key used for location procedure. And, for a roaming mobile station, location disclosure may be performed via a home network. Therefore, the second session key is limited to entities within the home network in the case of a roaming mobile station, since the location disclosure is performed via the home network.

A statement of Common Ownership was included with Applicants' remarks. Examiner does agree with applicants that a *prima facie* case for an obviousness rejection of claims 3, 28, and 33 cannot be maintained in the absence of Rowitch. As a result such rejection has been withdrawn.

Although not applied with this action Rowitch does read on all the independent claims, except for independent claims 24, 29, and 35. Applicants are respectfully invited to amend the independent claims by including the subject matter of dependent claims 3, 28, or 33 to eliminate Rowitch as prior art, since the inclusion of either of these claims would initiate a *prima facie* case for an obviousness rejection. And as described above

Art Unit: 2617

such case cannot be applied due to common ownership. Such amendment would only eliminate the use of Rowitch in future rejection. The claims would still be rejected under as described in the rejection session below.

A rejection using Rowitch is also applied to claims 36-45 below.

***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 36 and 43 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The above claims have been amended with the following limitation, “using a disclosure session key limited to entities within the home network.” Such limitation is not supported with the original disclosure, and therefore, constitutes new matter.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 5, 7-18, 20, 22-23, 30-32, 34-37, 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Papadimitriou et al. (Papadimitriou), U.S. Patent No. 6385458 in view of Cedervall et al. (Cedervall), US 20040203900 A1, Herle et al. (Herle), US 20030035544.

Regarding claims 1, 18, 22, 23, Papadimitriou discloses a apparatus, system, mobile station which includes an inherent processor, and medium (see claim 17 of the reference where a machine readable instructions executable by a computer is disclosed) of providing location services (LCS) (see abstract), comprising: receiving a request for location information for a mobile station (see col. 5, lines 56-67); performing location determination (i.e., performing first function) via a first set of at least one network entity to obtain location information for the mobile station (see col. 5, lines 56 -64; col. 6, lines 23-30); and performing location disclosure (i.e., performing a second function) via a second set of at least one network entity to provide the location information for the mobile station (see col. 6, lines 41-55); wherein the first function interacts with at least one peer first function located in a first set of at least one network entity to obtain the location information, and wherein the second function interacts with at least one peer second function located in a second set of at least one network entity to provide the location information (see col. 5, lines 56 -64; col. 6, lines 23-30; col. 6, lines 41-55).

Papadimitriou does disclose a method, apparatus, system, mobile station, and medium wherein a user request location information and determining whether present location information for the mobile station is available responsive to receiving request (see col. 5, lines 56-67).

Art Unit: 2617

Although Papadimitriou discloses performing location determination via a first set of at least one network entity to obtain location information for the mobile station, as described above, Papadimitriou does not specifically disclose the performing of the location determination procedure takes place when present location information is unavailable. Nor does it determining whether present location information is available from a cache; performing authorization for location determination based on a first security procedure; performing authentication for the location determination based on the first security procedure; performing authorization for location disclosure based on a second security procedure, independent of the first security procedure; performing authentication for the location disclosure based on the second security procedure, wherein the location determination step is skipped when the present location information for the mobile station is available from a cache.

However, Cedervall discloses a location manager that receives location requests from specific location-based service applications. Based on the received request, the location manager can access the location cache to determine whether any suitable location information is available for the identified wireless units and, if not, may invoke an LFE to obtain appropriate to obtain appropriate location information) (see paragraph 57).

Thus, Cedervall discloses determining whether present location information is available from a cache, and if not available, invoking an LFE (i.e., location finding equipment) to obtain (i.e., determine) appropriate location information.

Also, it should be noted that one skilled in the art would find it obvious that the invoking of the LFE would be skipped if location information is available from the cache.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Cedervall with the teachings as described by Papadimitriou to arrive at the claimed invention. A motivation for doing so would have been to provide the best available location information to the requesting entity which would also facilitate a fast response to the request.

The combination to Papadimitriou with Cedervall, however, does not specifically disclose performing authorization for location determination based on a first security procedure; performing authentication for the location determination based on the first security procedure; performing authorization for location disclosure based on a second security procedure, independent of the first security procedure; performing authentication for the location disclosure based on the second security procedure.

However, Herle discloses a requesting client access device transmits a request to a server over the internet. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit (i.e., disclose) the information in either an encrypted or decrypted form to the device (see abstract). Thus, by authenticating the requesting device, the server verifies whether the requesting device is authorized to receive the location information.

Thus, authentication and authorization processes are performed by the server in the disclosure of location information to a requesting device.

Furthermore, Herle discloses that the controller establish a secure connection with server using at least one encryption/decryption key, over the wireless network (see paragraph 8). Thus, an authentication takes place. In paragraph 36, it is disclosed that the

Art Unit: 2617

use of encryption-decryption keys enable the mobile station to its location out to those having authorization from the mobile station user. Therefore, one skilled in the art would find it obvious that since the server receives the location information from the mobile station in the location determination process, the server is authorized to receive such information, hence the authentication and authorization of the server.

It should also be disclosed that Herle discloses that the server determines the mobile station's location through various location techniques or by receiving the location information from the mobile station over an encrypted channel. Thus, the determining of the location information takes place by receiving the location information from the mobile station (see abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Herle with the teachings described by Papadimitriou and Cedervall to arrive at the claimed invention. A motivation for doing so would have been to make location information available to select individuals or organizations.

Regarding claim 5, Papadimitriou discloses a method (see claim 1 rejection), wherein the location determination and the location disclosure are performed in two separate LCS sessions (see col. 5, lines 56 -64 col. 6, lines 23-30; col. 6, lines 41-55).

Regarding claim 7, Papadimitriou discloses a method, wherein the first set of at least one network entity is located in a serving network for the mobile station (see col. 1, lines 66-67, and col. 2, lines 1-5) and the second set of at least one network entity is located in a home network for the mobile station (see col. 1, lines 45-57).

Regarding claim 8, Papadimitriou discloses a method, wherein the location

Art Unit: 2617

disclosure is performed by a location client and a location server (i.e., a method is disclosed in which a computer program has a location request module for receiving a location request from a user, a location request processing module that makes a location estimate with an accuracy based on a priority level associated with the user, and a terminal device location estimation reporting module that communicates the location estimate to the user) (see col. 4, lines 63-67, and col. 5, lines 1-2).

Regarding claim 9, Papadimitriou discloses a method, wherein the second set of at least one network entity includes an LCS provider (i.e., GMLC) (see col. 1, lines 60-65), and wherein the location client is located in the mobile station (i.e., as understood from the specification, the location client requests location information; with Papadimitriou discloses that the GMLC interfaces to users of a location service that is seeking the location of a mobile phone, one skilled in the art would unhesitatingly conceptualize that the location client is located in the mobile station) (see col. 1 lines 60-63).

Regarding claim 10, Papadimitriou and Cedervall disclose a method as described above (see claim 8 rejection).

Papadimitriou and Cedervall, however, do not specifically disclose a method wherein the second set of at least one network entity includes an LCS server, and wherein the location server is located in the mobile station or the LCS server.

However, Herle discloses a method wherein the second set of at least one network entity includes an LCS server, and wherein the location server is located in the mobile station or the LCS server (see abstract and fig. 3).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by the references to

Art Unit: 2617

arrive at the claimed invention. A motivation for doing so would have been to make location information available to select individuals and/or organizations.

Regarding claim 11, Papadimitriou discloses a method (refer to claim 1 reasoning), wherein the first set of at least one network entity includes a position determining entity (PDE) (i.e., LMU) (see col. 6, lines 28-30)

Regarding claim 12, Papadimitriou discloses a method (refer to claim 11 reasoning), wherein the first set of at least one network entity further includes a serving mobile positioning center (SMPC) (i.e., SMLC) (see col. 5, lines 5-9).

Regarding claim 13, Papadimitriou discloses a method as described in claim 11 reasoning.

Although Papadimitriou discloses a method as described above, Papadimitriou fails to specifically disclose a method wherein the first set of at least one network entity further includes a home authentication, authorization, and accounting (H-AAA) entity.

However, Papadimitriou discloses a method wherein at GMLC interfaces to users of a location service that is seeking the location of a mobile phone or other terminal device, performs user authorization tasks, and also forwards positioning requests to the mobile phone's current mobile network.

Therefore, (giving the fact that the GMLC performs user authorization tasks) it would have been obvious to one of ordinary skill at the time of the invention to modify the method so that it could include a home authentication, authorization, and accounting (H-AAA) entity. Such modification would have been considered a mere design consideration, which fails to patentably distinguish from the prior art.

Regarding claim 14, Papadimitriou discloses a method (refer to reasoning of

Art Unit: 2617

claim 1), wherein the second set of at least one network entity includes an LCS server (i.e., LCS algorithm) (see col. 5, lines 47-48).

Regarding claim 15, Papadimitriou discloses a method as described in claim 11 reasoning.

Although Papadimitriou discloses a method as described above, Papadimitriou fails to specifically disclose a method wherein the second set of at least one network entity further includes a home authentication, authorization, and accounting (H-AAA) entity.

However, Papadimitriou discloses a method wherein at GMLC interfaces to users of a location service that is seeking the location of a mobile phone or other terminal device, performs user authorization tasks, and also forwards positioning requests to the mobile phone's current mobile network.

Therefore, (giving the fact that the GMLC performs user authorization tasks) it would have been obvious to one of ordinary skill at the time of the invention to modify the method so that it could include a home authentication, authorization, and accounting (H-AAA) entity. Such modification would have been considered a mere design consideration, which fails to patentably distinguish from the prior art.

Regarding claim 16, Papadimitriou discloses a method as described in the reasoning of claim 1, wherein the location information for the mobile station comprises a location estimate for the mobile station (see abstract).

Regarding claim 17, Papadimitriou discloses a method as described in the reasoning of claim 1, wherein the location information for the mobile station comprises an uncertainty for the location estimate for the mobile station (i.e., Papadimitriou

Art Unit: 2617

discloses the primary task of the SMLC is to decide upon a positioning method to use to estimate the location of a mobile phone. Furthermore, knowing that estimation can be considered as a rough calculation, both uncertainty and accuracy may be comprised in estimation) (see col. 2, lines 5-8).

In paragraphs 36 and 38, Herle describes how the authentication/authorization process takes place. Encryption-decryption application is stored in a memory in order to compare any received keys with encryption-decryption keys.

Thus, one skilled in the art would find it obvious that the parties obtain key in order to establish or perform a session.

Therefore, the first secure LCS session takes place between the server and the mobile station.

Herle further discloses that a requesting client access device transmits a request to a server over the internet. The server authenticates the request to verify that the client access device is authorized to receive the location information (i.e., thus by authenticating the request, an authorization procedure is performed). If the client access device is authorized, the server can then transmit (i.e., disclose) the information in either an encrypted or decrypted form to the device (see abstract). Thus, by authenticating the requesting device, the server verifies whether the requesting device is authorized to receive the location information. If a request is received for location information for a particular mobile station, that request must contain a proper decryption key. Mobile station server application program determines if that decryption key is accurate so that the requesting entity can access the location information (see paragraph 44). Thus, one skilled in the art would find it obvious that a **second key setup** is performed to obtain an

Art Unit: 2617

encryption/decryption key for the secure disclosing of location information from the server.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Herle with the teachings described by Papadimitriou and Cedervall to arrive at the claimed invention. A motivation for doing so would have been to make location information available to select individuals or organizations.

Regarding claims 30 and 35, Papadimitriou discloses a method of providing location services (LCS), comprising: obtaining location information for a mobile station (i.e., a user requests the location of a terminal device; the LMUs return the location estimate to the GMLC in a LMU response step. Then in a report location estimate step, the GMLC sends the location estimate) (see col. 5, lines 56-57; col. 6, lines 51-56); providing the location information to a first application responsive to the first request (see col. 6, lines 41-55).

It should be noted that Papadimitriou further discloses that the GMLC interfaces to users of a location service that are seeking the location of a mobile station or other terminal device, and forwards positioning requests to the mobile phone's current network (see col. 1, lines 60-65).

Therefore, location information requests from a plurality of users are received and location information responses are provided to the plurality of users.

Therefore, Papadimitriou does read on the limitations of providing location information to a first application responsive to the first request for location information

Art Unit: 2617

for the mobile station and providing the location information to a second application (i.e., second requesting device) responsive to a second request (see col. 6, lines 41-55).

Although Papadimitriou discloses a method and apparatus as described, Papadimitriou does not specifically disclose a method and apparatus comprising performing authorization for location determination responsive to a first request for location information based on a first security procedure; authenticating messages between a mobile station and a serving network based on a first session obtained in the first security procedure; obtaining location information when present location information for the mobile station is unavailable from a cache; performing authorization for location disclosure responsive to the first request for location information based on a second security procedure, independent of the first security procedure; and skipping the obtaining the location information when the present location information for the mobile station is available from the cache; performing authorization for location disclosure responsive to a second request for location information based on the second security procedure; authenticating location disclosure messages exchanged between the mobile station and a home network using a second session obtained in the second security procedure; and skipping the obtaining the suitable location information when the present, location information for the mobile station is available from the cache.

However, Cedervall discloses a location manager that receives location requests from specific location-based service applications. Based on the received request, the location manager can access the location cache to determine whether any suitable location information is available for the identified wireless units and, if not, may invoke

Art Unit: 2617

an LFE to obtain appropriate to obtain appropriate location information) (see paragraph 57).

Thus, Cedervall discloses determining whether present location information is available from a cache, and if not available, invoking an LFE (i.e., location finding equipment) to obtain (i.e., determine) appropriate location information.

Also, it should be noted that one skilled in the art would find it obvious that the invoking of the LFE would be skipped if location information is available from the cache. And, if location information is available from the cache, different received location requests would be served by location information obtained from the cache. Thus, different location disclosure procedures would be realized with only a single location determination (i.e., determining whether location information is available from the cache).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Cedervall with the teachings as described by Papadimitriou to arrive at the claimed invention. A motivation for doing so would have been to provide the best available location information to the requesting entity which would also facilitate a fast response to the requests.

The combination to Papadimitriou with Cedervall, however, does not specifically disclose performing authorization for location determination responsive to a first request for location information based on a first security procedure; authenticating messages between a mobile station and a serving network based on a first session obtained in the first security procedure; performing authorization for location disclosure responsive to the first request for location information based on a second security procedure,

Art Unit: 2617

independent of the first security procedure; performing authorization for location disclosure responsive to a second request for location information based on the second security procedure; authenticating location disclosure messages exchanged between the mobile station and a home network using a second session obtained in the second security procedure.

First, it should be noted, that the different location disclosures are associated with the different requests. Thus, each time that a location request is submitted, a new location disclosure is performed; hence a new authorization and authentication processes are performed.

Herle discloses a MS location server that may periodically or aperiodically receive access **requests from client access devices**. MS location server then authenticates the client access devices using user name and password verification procedures. If the client devices properly authenticate, MS location server transmits the MS position data to the client access device (see paragraph 50).

More particularly, Herle discloses a requesting client access device transmits a request to a server over the internet. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit (i.e., disclose) the information in either an encrypted or decrypted form to the device (see abstract). Thus, by authenticating the requesting device, the server verifies whether the requesting device is authorized to receive the location information.

Thus, authentication and authorization processes are performed by the server in the disclosure of location information to a requesting device.

Furthermore, Herle discloses that the controller establish a secure connection with server using at least one encryption/decryption key, over the wireless network (see paragraph 8). Thus, an authentication takes place. In paragraph 36, it is disclosed that the use of encryption-decryption keys enable the mobile station to its location out to those having authorization from the mobile station user. Therefore, one skilled in the art would find it obvious that since the server receives the location information from the mobile station in the location determination process, the server is authorized to receive such information, hence the authentication and authorization of the server.

It should also be disclosed that Herle discloses that the server determines the mobile station's location through various location techniques or by receiving the location information from the mobile station over an encrypted channel. Thus, the determining of the location information takes place by receiving the location information from the mobile station (see abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Herle with the teachings described by Papadimitriou and Cedervall to arrive at the claimed invention. A motivation for doing so would have been to make location information available to select individuals or organizations.

Regarding claim 31, Papadimitriou discloses a method (see claim 30 rejection) wherein the location information is obtained by performing location determination once via one location determination session (see col. 5, lines 56 -64; col. 6, lines 23-30); wherein the location information is provided to the first and second applications by performing location disclosure twice via two location disclosure sessions (i.e., providing

Art Unit: 2617

location information to different users) (see col. 5, lines 56-57; col. 6, lines 51-56). Also refer to Cedervall wherein it is disclosed determination whether location information is available from a cache, and if not, invoking an LFE to obtain appropriate location information (see paragraph 57). Different location information regarding wireless units may be received, and from these requests, only when location information is not available from the cache would the LFE be invoked. Therefore, plurality requests may be served by location information retrieved from the cache (i.e., one location determination, plurality of location disclosures to a plurality of request entities).

As stated in the rejection of claim 30, a reason to combine Papadimitriou with Cedervall would have been to provide the best available location information to the requesting entity which would also facilitate a fast response to the requests.

Regarding claims 32 and 42, Papadimitriou discloses a method (refer to claims 30 and 36 rejections) further comprising: caching the location information in mobile station or a network entity (i.e., Papadimitriou discloses an MSC in both the originating and the destination networks which include a VLR for maintaining a register of information (location information is stored in the register) for all mobile phone currently served by the respective network) (see col. 1, lines 49-65). Also refer to Cedervall which discloses a location platform within a wireless network that may contain a location information cache that includes stored location information (see paragraph 22).

Regarding claim 34, Papadimitriou discloses a method (refer to claim 30 reasoning) wherein the first application is located in a first network (see col. 1, lines 41-47) and the second application is located in a second network (see col. 2, lines 18-25).

Regarding claims 36 and 43, Papadimitriou discloses an apparatus and method of

Art Unit: 2617

providing location services (LCS), comprising: receiving a request for location information for a mobile station (see col. 5, lines 56-67); performing location determination via at least one network entity in a serving network to obtain desirable location information for a mobile station (see col. 1, lines 66-67, and col. 2, lines 1-5; col. 5, lines 56 -64; col. 6, lines 23-30); and performing location disclosure via at least one network entity in a home network to provide the desirable location information for the mobile station (see col. 1, lines 45-57; col. 6, lines 41-55).

Papadimitriou, however, does not specifically disclose an apparatus and method comprising determining whether present location information is available from a cache, performing authorization for location determination based on a first security procedure; performing location determination when present location information is unavailable from a cache; performing authorization for location disclosure based on a second security procedure, independent of the first security procedure; performing location information using a disclosure session key limited to entities within the home network, and skipping the location determination when the present location information for the mobile station is available from the cache.

However, Cedervall discloses a location manager that receives location requests from specific location-based service applications. Based on the received request, the location manager can access the location cache to determine whether any suitable location information is available for the identified wireless units and, if not, may invoke an LFE to obtain appropriate to obtain appropriate location information) (see paragraph 57).

Art Unit: 2617

Thus, Cedervall discloses determining whether present location information is available from a cache, and if not available, invoking an LFE (i.e., location finding equipment) to obtain (i.e., determine) appropriate location information.

Also, it should be noted that one skilled in the art would find it obvious that the invoking of the LFE would be skipped if location information is available from the cache since the invoking only take place if location information is not available from the cache.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Cedervall with the teachings as described by Papadimitriou to arrive at the claimed invention. A motivation for doing so would have been to provide the best available location information to the requesting entity which would also facilitate a fast response to the request.

The combination to Papadimitriou with Cedervall, however, does not specifically performing authorization for location determination based on a first security procedure; performing authorization for location disclosure based on a second security procedure, independent of the first security procedure; performing location information using a disclosure session key limited to entities within the home network.

However, Herle discloses a requesting client access device transmits a request to a server over the internet. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit (i.e., disclose) the information in either an encrypted or decrypted form to the device (see abstract). Thus, by authenticating the requesting device, the server verifies whether the requesting device is authorized to receive the location information.

Thus, authentication and authorization processes are performed by the server in the disclosure of location information to a requesting device.

Furthermore, Herle discloses that the controller establish a secure connection with server using at least one encryption/decryption key, over the wireless network (see paragraph 8). Thus, an authentication takes place. In paragraph 36, it is disclosed that the use of encryption-decryption keys enable the mobile station to its location out to those having authorization from the mobile station user. Therefore, one skilled in the art would find it obvious that since the server receives the location information from the mobile station in the location determination process, the server is authorized to receive such information, hence the authentication and authorization of the server.

It should also be disclosed that Herle discloses that the server determines the mobile station's location through various location techniques or by receiving the location information from the mobile station over an encrypted channel. Thus, the determining of the location information takes place by receiving the location information from the mobile station (see abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Herle with the teachings described by Papadimitriou and Cedervall to arrive at the claimed invention. A motivation for doing so would have been to make location information available to select individuals or organizations.

6. Claims 3, 4, 20, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Papadimitriou, Cedervall, and Herle, further in view of Horn et al.

Art Unit: 2617

(Horn), U.S. Patent No. 6064741.

Regarding claim 3, the combination discloses a method as described in claim 1 reasoning.

Although the combination discloses a method as recited above, the combination does not specifically disclose a method, wherein the first security procedure is based on an MD-5 algorithm and the second security procedure is based on an Authentication and Key Agreement (AKA) procedure.

However, Horn discloses security measures based on both MD-5 algorithm and Authentication and Key Agreement (AKA) (see col. 3, lines 44-50; col. 5, lines 20-41).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described to arrive at the claimed invention. A motivation to do so would have been to insure the security of the location determination/disclosure procedure.

Regarding claims 4, 20, and 37, the combination of Papadimitriou with Cedervall discloses an apparatus and method as described (see claims 1, 18, and 36 rejections).

The combination, however, does not specifically disclose an apparatus and method further comprising performing a first session key setup to obtain a first session key, wherein the first session key is used for authentication and encryption of messages exchanged with the first set of at least one network entity; and performing a second session key setup to obtain a second session key for use as the disclosure session key, wherein the second key is used for authentication and encryption of messages exchanged with the second set of at least one network entity.

However, Herle discloses a mobile station that uses at least one

Art Unit: 2617

encryption/decryption key to establish a connection with a server (i.e., location determination using key to authenticate and authorize the organization) (see paragraph 8).

In paragraphs 36 and 38, Herle describes how the authentication/authorization process takes place. Encryption-decryption application is stored in a memory in order to compare any receives keys with encryption-decryption keys.

Thus, one skilled in the art would find it obvious that the parties (i.e., session between the location server and the mobile station, and between the requesting device and the server) obtain key in order to establish or perform a session.

Therefore, the first secure LCS session take place between the server and the mobile station.

Herle further discloses that a requesting client access device transmits a request to a server over the internet. The server authenticates the request to verify that the client access device is authorized to receive the location information (i.e., thus by authenticating the request, an authorization procedure is performed). If the client access device is authorized, the server can then transmit (i.e., disclose) the information in either an encrypted or decrypted form to the device (see abstract). Thus, by authenticating the requesting device, the server verifies whether the requesting device is authorized to receive the location information. If a request is received for location information for a particular mobile station, that request must contain a proper decryption key. Mobile station server application program determines if that decryption key is accurate so that the requesting entity can access the location information (see paragraph 44). Thus, one skilled in the art would find it obvious that a **second key setup** is performed to obtain an

Art Unit: 2617

encryption/decryption key for the secure disclosing of location information from the server.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Herle with the teachings described by Papadimitriou and Cedervall to arrive at the claimed invention. A motivation for doing so would have been to make location information available to select individuals or organizations.

Note: one skilled in the art would appreciate that all the parties in the session have obtained a key for authentication and encryption.

However, Papadimitriou in combination with Cedervall and Herle do not specifically disclose performing session keys setup to obtain session keys.

However, Horn discloses a method wherein session key K is calculated by the bit-by-bit application of the exclusive-OR function to the first interim key K1 and the second interim key K2. A first response A is formed by encoding a user constant, which is known both to the user computer and to the network computer unit, with the session key using a function a symmetric cryptographic function or a hash function or a one-way function (see col. 5, lines 20-27).

Thus, one skilled in the art would appreciate that session keys setup may be performed to obtain session keys which may be used for authentication and encryption.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described to arrive at the claimed invention. A motivation to do so would have been to insure the security of the location determination/disclosure procedure.

7. Claims 24-26, 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Papadimitriou, Cedervall, and Herle, further in view of Horn.

Regarding claims 24 and 29, Papadimitriou discloses an apparatus and method of providing location services (LCS) (see abstract), comprising: receiving a request for location information for the mobile station (see col. 5, lines 56-67); performing location determination via a first LCS session to obtain location information for the mobile station responsive to the request (see col. 5, lines 56-64; col. 6, lines 23-30); and performing location disclosure via a second LCS session to provide the location information for the mobile station responsive to the request for the location information (see col. 6, lines 41-55).

Papadimitriou, however, does not specifically disclose a method, apparatus, system, mobile station, and medium wherein performing location determination takes place when the present location information for the mobile station is unavailable from a cache and skipping the location determination when the present location information for the mobile station is available from the cache. Nor does it disclose performing a first session key setup to obtain a first session key, wherein the first session key is used for authentication and encryption of messages exchanged with the at least one network entity in the serving network; and performing a second session key setup to obtain a second session key, wherein the second session key is used for authentication and encryption of messages exchanged with the at least one network entity in the home network.

However, Cedervall discloses a location manager that receives location requests from specific location-based service applications. Based on the received request, the

Art Unit: 2617

location manager can access the location cache to determine whether any suitable location information is available for the identified wireless units and, if not, may invoke an LFE to obtain appropriate to obtain appropriate location information) (see paragraph 57).

Thus, Cedervall discloses determining whether present location information is available from a cache, and if not available, invoking an LFE (i.e., location finding equipment) to obtain (i.e., determine) appropriate location information.

Also, it should be noted that one skilled in the art would find it obvious that the invoking of the LFE would be skipped if location information is available from the cache.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Cedervall with the teachings as described by Papadimitriou to arrive at the claimed invention. A motivation for doing so would have been to provide the best available location information to the requesting entity which would also facilitate a fast response to the request.

The combination of Papadimitriou and Cedervall, however, does not specifically disclose a method and apparatus, further comprising: performing a first session key setup to obtain a first session key, wherein the first session key is used for authentication and encryption of messages exchanged with the at least one network entity in the serving network; and performing a second session key setup to obtain a second session key, wherein the second session key is used for authentication and encryption of messages exchanged with the at least one network entity in the home network.

However, Herle discloses a mobile station that uses at least one encryption/decryption key to establish a connection with a server (i.e., location

Art Unit: 2617

determination using key to authenticate and authorize the organization) (see paragraph 8).

In paragraphs 36 and 38, Herle describes how the authentication/authorization process takes place. Encryption-decryption application is stored in a memory in order to compare any received keys with encryption-decryption keys.

Thus, one skilled in the art would find it obvious that the parties (i.e., session between the location server and the mobile station, and between the requesting device and the server) obtain key in order to establish or perform a session.

Therefore, the first secure LCS session takes place between the server and the mobile station.

Herle further discloses that a requesting client access device transmits a request to a server over the internet. The server authenticates the request to verify that the client access device is authorized to receive the location information (i.e., thus by authenticating the request, an authorization procedure is performed). If the client access device is authorized, the server can then transmit (i.e., disclose) the information in either an encrypted or decrypted form to the device (see abstract). Thus, by authenticating the requesting device, the server verifies whether the requesting device is authorized to receive the location information. If a request is received for location information for a particular mobile station, that request must contain a proper decryption key. Mobile station server application program determines if that decryption key is accurate so that the requesting entity can access the location information (see paragraph 44). Thus, one skilled in the art would find it obvious that a **second key setup** is performed to obtain an encryption/decryption key for the secure disclosing of location information from the server.

Art Unit: 2617

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Herle with the teachings described by Papadimitriou and Cedervall to arrive at the claimed invention. A motivation for doing so would have been to make location information available to select individuals or organizations.

Note: one skilled in the art would appreciate that all the parties in the session have obtained a key for authentication and encryption.

However, Papadimitriou in combination with Cedervall and Herle do not specifically disclose performing session keys setup to obtain session keys.

However, Horn discloses a method wherein session key K is calculated by the bit-by-bit application of the exclusive-OR function to the first interim key K1 and the second interim key K2. A first response A is formed by encoding a user constant, which is known both to the user computer and to the network computer unit, with the session key using a function a symmetric cryptographic function or a hash function or a one-way function (see col. 5, lines 20-27).

Thus, one skilled in the art would appreciate that session keys setup may be performed to obtain session keys which may be used for authentication and encryption.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described to arrive at the claimed invention. A motivation to do so would have been to insure the security of the location determination/disclosure procedure.

Regarding claim 25, Papadimitriou discloses a method (refer to reasoning of claim 24), wherein the first and second LCS sessions are performed at different times

Art Unit: 2617

(see col. 5, lines 56 -64; col. 6, lines 23-30; col. 6, lines 41-55).

Regarding claim 26, the combination of Papadimitriou with Fitch discloses a method as described above (see claim 24 rejection).

The combination of Papadimitriou and Cedervall, however, does not specifically disclose method, apparatus, system, mobile station, and medium comprising performing authorization for location determination based on a first security procedure; performing authorization for location disclosure based on a second security procedure.

However, Herle discloses a requesting client access device transmits a request to a server over the internet. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit (i.e., disclose) the information in either an encrypted or decrypted form to the device (see abstract). Thus, by authenticating the requesting device, the server verifies whether the requesting device is authorized to receive the location information.

Thus, it is clear that authorization process is performed by the server in the disclosure of location information to a requesting device.

Furthermore, Herle discloses that the controller establish a secure connection with server using at least one encryption/decryption key, over the wireless network (see paragraph 8).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Herle with the teachings described by Papadimitriou and Fitch to arrive at the claimed invention. A

Art Unit: 2617

motivation for doing so would have been to make location information available to select individuals or organizations.

8. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Papadimitriou, Cedervall, and Herle, further in view of Deloach (previously disclosed).

Regarding claim 28, the combination discloses a method as described above (refer to claim 24 reasoning).

Although the combination discloses a method as recited above, the combination does not specifically disclose a method, further comprising: providing a first call detail record (CDR) for the first LCS session; and providing a second CDR for the second LCS session.

However, Deloach discloses a method for the determination of the positions of wireless mobile stations in a mobile communication network, in which When there is a physical change in the cellular infrastructure or in the cellular infrastructure configuration, the base station almanac data base server maintains records in the base station almanac data base reflecting both the old and new conditions until all of the PDEs are switched over to the new conditions (see page 2, paragraph 16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described, which are analogous art because they are from the same field of endeavor, to arrive at the claimed invention. A motivation to do so would have been to ensure accuracy and completeness of the record.

Art Unit: 2617

9. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Papadimitriou, Cedervall, and Herle, further in view of Deloach (previously disclosed).

Regarding claim 33, the combination discloses a method as described above (refer to claim 30 reasoning).

Although the combination discloses a method as recited above, the combination does not specifically disclose a method, further comprising: providing a first call detail record (CDR) for providing the location information to the first application; and providing a second CDR for providing the location information to the second application.

However, Deloach discloses a method for the determination of the positions of wireless mobile stations in a mobile communication network, in which When there is a physical change in the cellular infrastructure or in the cellular infrastructure configuration, the base station almanac data base server maintains records in the base station almanac data base reflecting both the old and new conditions until all of the PDEs are switched over to the new conditions (see page 2, paragraph 16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described, which are analogous art because they are from the same field of endeavor, to arrive at the claimed invention. A motivation to do so would have been to ensure accuracy and completeness of the record.

10. Claims 38-40 rejected under 35 U.S.C. 103(a) as being unpatentable over Papadimitriou, Cedervall, and Herle, further in view of Haverinen et al. (Haverinen), Pub. No. 2003/0119481.

Regarding claim 38, the combination discloses a method as described above (refer

Art Unit: 2617

to claim 36 reasoning), wherein the at least one network entity in the serving network includes a serving mobile positioning center (SMPC) (i.e., SMLC) (see Papadimitriou col. 5, lines 5-9).

Although the combination discloses a method as described above, the combination does not specifically disclose a method further comprising: determining an Internet Protocol (IP) address of the SMPC.

However, Haverinen discloses a method wherein after the MS has selected a PLMN, it can transmit a request to the local network BAN for setting up a connection with a network element according to the network element identifier linked with the identifier of the selected PLMN. The local network BAN finds out the IP address of the network element (see page 4, paragraph 43).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the described teachings, which are analogous, to arrive at the claimed invention. A motivation to do so would have been to provide a proper arrangement for the request procedure.

Regarding claim 39, the combination discloses a method as described in claim 36 reasoning (refer to claim 36 and 38 reasoning).

Although the combination discloses a method as described above, the combination does not specifically disclose a wherein the IP address of the SMPC is determined using a fully qualified domain name for the SMPC.

However, Haverinen discloses a method wherein The local network BAN finds out the IP address of the network element from the network identifier, which is typically a domain name, (see page 4, paragraph 43).

Art Unit: 2617

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the described teachings, which are analogous, to arrive at the claimed invention. A motivation to do so would have been to provide a proper arrangement for the request procedure.

Regarding claim 40, Papadimitriou discloses a method (refer to claims 36, and 38 reasoning) wherein the location disclosure is performed via the SMPC (i.e., the GMLC communicates with a Serving Mobile Location Center (SMLC) via Mobile Application Part (MAP) messaging. The SMLC (i.e. SMPC) provides the network resources needed to process calls in the network, and particularly to locate a mobile phone, and is directly associated with the MSC communicating with a mobile station that is being located) (see col. 1, line 66-67; col. 2, lines 1-5).

11. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cedervall in view of Herle.

Regarding claim 44, Cedervall discloses a method of providing location services comprising: receiving a request for location disclosure (i.e., location manager receives location requests) (see paragraph 52); determining whether cached location information is available, if the cached location information is available, responding to the request for location disclosure with location information, if the location information is not available, initiating a request for location determination (i.e., a location manager that receives location requests from specific location-based service applications. Based on the received request, the location manager can access the location cache to determine whether any suitable location information is available for the identified wireless units and, if not, may

Art Unit: 2617

invoke an LFE to obtain appropriate to obtain appropriate location information (see paragraph 57). Thus, Cedervall discloses determining whether present location information is available from a cache, and if not available, invoking an LFE (i.e., location finding equipment) to obtain (i.e., determine) appropriate location information. Also, it should be noted that one skilled in the art would find it obvious that the invoking of the LFE would be skipped if location information is available from the cache), and communicating location information (see paragraph 59. Also refer to paragraphs 53-58).

Cedervall, however, does not specifically disclose a method comprising authenticating and authorizing the request using a secure disclosure session key and a secure disclosure session, responding to the request in a secure session, establishing a secure determination session, independent of the secure disclosure session, and communicating location information within the secure determination session.

However, Herle discloses a requesting client access device transmits a request to a server over the internet. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit (i.e., disclose) the information in either an encrypted or decrypted form to the device (see abstract). Thus, by authenticating the requesting device, the server verifies whether the requesting device is authorized to receive the location information.

Thus, authentication and authorization processes are performed by the server in the disclosure of location information to a requesting device.

Furthermore, Herle discloses that the controller establish a secure connection with server using at least one encryption/decryption key, over the wireless network (see

Art Unit: 2617

paragraph 8). Thus, an authentication takes place. In paragraph 36, it is disclosed that the use of encryption-decryption keys enable the mobile station to its location out to those having authorization from the mobile station user. Therefore, one skilled in the art would find it obvious that since the server receives the location information from the mobile station in the location determination process, the server is authorized to receive such information, hence the authentication and authorization of the server.

It should also be disclosed that Herle discloses that the server determines the mobile station's location through various location techniques or by receiving the location information from the mobile station over an encrypted channel. Thus, the determining of the location information takes place by receiving the location information from the mobile station (see abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Herle with the teachings described by Papadimitriou and Cedervall to arrive at the claimed invention. A motivation for doing so would have been to make location information available to select individuals or organizations.

12. Claim 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cedervall and Herle, further in view of Horn (previously disclosed).

Regarding claim 45, Cedervall discloses a method as described (see claim 44 rejection).

Herle does disclose a method wherein a controller is capable of establishing a secure connection with location server using at least one encryption/decryption key over

Art Unit: 2617

the wireless network over which the geographical location information is transmitted (see paragraph 8). Furthermore, Herle discloses that request for location information received from a requesting device must contain a proper decryption key, and a determination is performed to verify whether the decryption key is accurate (see paragraph 44). Therefore, secure communication is performed between a requesting device and the server, and between the server and the mobile station.

However, the combination of Cedervall with Herle does not specifically disclose receiving a request for the secure disclosure session key; and providing the secure disclosure key in response to successful authentication and validation of the request for the secure session key.

However, Horn discloses a method for the exchange of cryptographic keys in a network computer unit and in a user computer unit, in which the following security mechanism is realized: agreement on the key between the user and the network with mutual implicit authentication, i.e. the method achieves the effect that, after completion of the procedure, a joint secret session key is available, of which each party knows that only the authentic counterpart can likewise be in possession of the secret session key (i.e., authentication and key agreement) (see col. 3, lines 44-50). Furthermore, a session key is calculated by the bit-by-bit application of the exclusive-OR function to the first interim key and the second interim key. A first response is formed by encoding a user constant, which is known both to the user computer and to the network computer unit, with the session key using a symmetric cryptographic function or a hash function or a one-way function. MD5 algorithm is a known hash function (see col. 5, lines 20-41).

Thus, one skilled in the art would appreciate that a request for a session key is

Art Unit: 2617

received and based on that request, a session key is provided after implicit authentication.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described to arrive at the claimed invention. A motivation to do so would have been to insure the security of the location determination/disclosure procedure.

***Claim Rejections - 35 USC § 102***

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. Claims 36-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Rowitch et al (Rowitch), US 20040248551 A1

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention “by another,” or by an appropriate showing under 37 CFR 1.131.

Art Unit: 2617

Regarding claims 36 and 43, Rowitch discloses a method and apparatus of providing location services (LCS) (see abstract), comprising: receiving a request for location information for a mobile station (i.e., sending a request for positioning to the MPC) (see paragraph 31); determining whether present location information is available from a cache (i.e., the MPC checks to see whether there is a need for the position location engine to determine the position of the mobile station. That is there are instances in which a cached position for the mobile station may be used rather than having to recalculate the location of the mobile station) (see paragraph 36); performing authorization for location determination based on a first security procedure (i.e., location determination may utilize a first security procedure for authorization and to obtain a first session key used for location determination) (see abstract); performing location determination via a first set of at least one network entity in a serving network to obtain location information for the mobile station responsive to the request for the location information when present location information for the mobile station is unavailable (see abstract and paragraphs 36-37); performing authorization for location disclosure based on a second security procedure, independent of the first security procedure (i.e., location disclosure may utilize a second security procedure for authorization and to obtain a second session key used for location disclosure) (see abstract); and performing location disclosure via a second set of at least one network entity in a home network to provide the location information for the mobile station responsive to the request for the location information using a disclosure session key limited to entities within the home network (i.e., location disclosure may be performed via a second set) (see abstract), and skipping the location determination when the present location information for the mobile station is available

Art Unit: 2617

from the cache (i.e., the MPC checks to see whether there is a need for the position location engine to determine the position of the mobile station. That is there are instances in which a cached position for the mobile station may be used rather than having to recalculate the location of the mobile station (see abstract and paragraph 36). Inherently, if location information is available from the cache, the position location engine will not be needed to determine the position of the mobile station). Also, Rowitch discloses that location disclosure utilizes a second session key utilize a second security procedure for authorization and to obtain a session key used for location procedure. And, for a roaming mobile station, location disclosure may be performed via a home network. Therefore, the second session key is limited to entities within the home network in the case of a roaming mobile station, since the location disclosure is performed via the home network.

Regarding claim 37, Rowitch discloses a method and apparatus (see claim 36 rejection) further comprising performing a first session key setup to obtain a first session key, wherein the first session key is used for authentication and encryption of messages exchanged with the first set of at least one network entity (see abstract); and performing a second session key setup to obtain a second session key for use as the disclosure session key, wherein the second session key is used for authentication and encryption of messages exchanged with the second set of at least one network entity (see abstract).

Regarding claim 38, Rowitch discloses a method (see claim 36 rejection) wherein the at least one network entity in the serving network includes a serving mobile positioning center (SMPC) (see paragraphs 31-32), the method further comprising determining an Internet Protocol (IP) address of the SMPC (i.e., IP address) (see paragraph 32).

Art Unit: 2617

Regarding claim 39, Rowitch discloses a method (see claim 38 rejection) wherein the IP address of the SMPC is determined using a fully qualified domain name (URL) for the SMPC (see paragraphs 31-32).

Regarding claim 40, Rowitch discloses a method (see claim 38 rejection) wherein the location disclosure is performed via the SMPC (see paragraphs 32 and 36).

Regarding claim 41, Rowitch discloses a method (see claim 36 rejection) further comprising: sending a message to the mobile station to trigger the mobile station to initiate a LCS session for performing location determination (i.e., the mobile station is notified that the LBS application is attempting to run) (see paragraph 30).

Regarding claim 42, Rowitch discloses a method (see claim 36 rejection) further comprising: caching the location information in the mobile station, a network entity in the serving network, a network entity in the home network, or a combination thereof (see abstract)

Regarding claim 44, Rowitch discloses a method of providing location services (LCS), comprising: receiving a request for location disclosure (i.e., sending a request for positioning to the MPC) (see paragraph 31); authenticating and authorizing the request using a secure disclosure session (see abstract and paragraph 36); determining whether cached location information is available (see paragraph 36); if the cached location information is available, responding to the request for location disclosure with the location information in the secure disclosure session (see paragraph 36); if the cached location information is not available, initiating a request for location determination (see paragraph 37); establishing a secure determination session, independent of the secure

Art Unit: 2617

disclosure session (see abstract and paragraphs 37 and 53); and communicating location information within the secure determination session (see paragraphs 37 and 53).

Regarding claim 45, Rowitch discloses a method (see claim 44 rejection) wherein authenticating and authorizing the request comprises receiving a request for a secure disclosure session key and providing the secure disclosure session key in response to successful authentication and validation of the request for the secure session key (see abstract).

### ***Conclusion***

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PIERRE-LOUIS DESIR whose telephone number is (571)272-7799. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dwayne Bost can be reached on (571)272-7023. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Art Unit: 2617

Customer Service Representative or access to the automated information system, call  
800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PIERRE-LOUIS DESIR/  
Examiner, Art Unit 2617